UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,127	03/01/2002	Yves Audebert	L741.02102	2740

24257	7590	08/03/2006		

STEVENS DAVIS MILLER & MOSHER, LLP
1615 L STREET, NW
SUITE 850
WASHINGTON, DC 20036

EXAMINER
HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

1   This action is in response to the communication filed on 5/15/2006.

2   **DETAILED ACTION**

3   *Response to Arguments*

4   Applicants' arguments filed 5/15/2006 have been fully considered but they are not

5   persuasive. Applicants' argue, with regards to the independent claims, primarily that Davis did

6   not disclose a local client and a first server that have a first component for mutual authentication.

7   In response to applicant's argument that the references fail to show certain features of applicant's

8   invention, it is noted that the features upon which applicant relies are not recited in the rejected

9   claim(s). Although the claims are interpreted in light of the specification, limitations from the

10   specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26

11   USPQ2d 1057 (Fed. Cir. 1993). As such the examiner does not find the argument persuasive,

12   and has maintained the prior art rejections presented in the communication dated 1/17/2006.

13   Claims 1-31 have been examined.

14   *Claim Rejections - 35 USC § 102*

15   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

16   basis for the rejections under this section made in this Office action:

17   *A person shall be entitled to a patent unless –*

18   *(b) the invention was patented or described in a printed publication in this or a foreign country*
19   *or in public use or on sale in this country, more than one year prior to the date of application for*
20   *patent in the United States.*
21

22   Claims 1-2, 4, 8-16, 19-20, 24-28, and 31 are rejected under 35 U.S.C. 102(b) as being

23   anticipated by Davis et al. (US Patent Number 6,105,008) hereinafter referred to as Davis.

1   Regarding claim 1, Davis disclosed a post issuance system for performing data or

2   configuration changes within a personal security device (PSD) (Stored-Value Card See Davis

3   Fig. 1), said system comprising: said PSD, including at least one functional application (See

4   Davis Fig. 1 and Col. 1 Lines 45-49) and a PSD cryptographic component (See Davis Fig. 1

5   Element 22), a local client functionally connected to said PSD (See Davis Fig. 4 Element 204), a

6   first server functionally connected to said local client (See Davis Fig. 4 Element 206), said PSD

7   and said first server comprising a first component for mutual authentication (See Davis Col. 13

8   Line 47 – Col. 14 Line 13), at least one hardware security module (HSM), including an HSM

9   cryptographic component complementary to said PSD cryptographic component, said at least

10   one HSM being functionally connected to said first server (See Davis Fig. 4 Element 218 and

11   Col. 14 Lines 14-38), a communications pipe, established between said PSD and said at least one

12   HSM (See Davis Col. 13 Line 47 – Col. 14 Line 13), and a storage component that stores or

13   generates said data or configuration changes, said storage component being functionally

14   connected to said first server (See Davis Fig. 11D), wherein: said at least one HSM comprises a

15   controlling component that controls said data or configuration changes sent through said

16   communications pipe to said PSD (See Davis Fig. 11D).

17   Regarding claim 19, Davis disclosed a post issuance method for performing data or

18   configuration changes within a personal security device (PSD) (Stored-Value Card See Davis

19   Fig. 1), said method comprising: establishing a communications pipe between said PSD and at

20   least one hardware security module (HSM) (See Davis Col. 13 Line 47 – Col. 14 Line 13),

21   wherein said PSD is functionally connected to a local client (See Davis Fig. 4 Element 204) and

22   said at least one HSM is functionally connected to a first server (See Davis Fig. 4 Element 218

1   and Col. 14 Lines 14-38), mutually authenticating said PSD and said first server (See Davis Col.

2   13 Line 47 – Col. 14 Line 13), selecting at least one functional application within said PSD

3   associated with existing data or configurations (See Davis Fig. 1 and Col. 1 Lines 45-49),

4   generating or retrieving an HSM cryptographic component complementary to a cryptographic

5   component included inside said PSD (See Davis Fig. 4 Element 218 and Col. 14 Lines 14-38),

6   retrieving said data or configuration changes, processing said data or configuration changes by

7   said first server (See Davis Col. 13 Paragraph 3), encrypting said processed data or configuration

8   changes by said at least one HSM using said complementary HSM cryptographic component

9   (See Davis Col. 15 Line 27 – Col. 16 Line 33 and Fig. 11D), routing said encrypted processed

10   data or configuration changes through said communications pipe into said PSD (See Davis Col.

11   13 Paragraphs 3-4), and decrypting and processing said processed data or configuration changes

12   by said at least one functional application using said PSD cryptographic component (See Davis

13   Col. 13 Paragraph 5).

14   Regarding claim 2, Davis disclosed a network for the establishment of said

15   communications pipe (See Davis Fig. 4).

16   Regarding claims 4, and 20, Davis disclosed at least one second server in processing

17   communications with said first server, wherein said at least one second server includes stored

18   data or configuration changes retrievable using a PSD unique identifier (See Davis Fig. 4

19   Element 208, Col. 12 Paragraph 1 and Col. 15 Paragraph 2).

20   Regarding claim 8, Davis disclosed a network for the establishment of said

21   communications pipe and for functionally connecting said at least one second server to said first

22   server, and sending means for sending said retrieved data or configuration changes from said at

1   least one second server over said network to said first server (See Davis Fig. 4 and Col. 12

2   Paragraph 1 – Col. 13 Paragraph 3).

3   Regarding claim 9, Davis disclosed that said first server comprises first processing means

4   for receiving and processing said data or configuration changes, and wherein said at least one

5   HSM comprises second processing means for further processing said data or configuration

6   changes (See Davis Col. 13 Paragraph 3 and Col. 15 Paragraph 3 – Col. 16 Paragraph 2).

7   Regarding claim 10, Davis disclosed that said at least one HSM comprises generating

8   means for generating at least one command executable by said at least one functional application

9   (See Col. 15 Line 63 – Col. 16 Line 33).

10   Regarding claim 11, Davis disclosed that said at least one HSM comprises encrypting

11   means for encrypting said at least one command and said data or configuration changes, forming

12   at least one cryptogram (See Davis Col. 16 Lines 20-22).

13   Regarding claim 12, Davis disclosed sending means for sending said at least one

14   cryptogram through said communications pipe into said PSD for processing by said at least one

15   functional application (See Davis Col. 16 Paragraph 2 and Col. 13 Lines 41-63).

16   Regarding claim 13, Davis disclosed that said at least one functional application

17   comprises decrypting means for decrypting said cryptogram using said PSD cryptographic

18   means, and executing means for executing said at least one command (See Davis Col. 13 Lines

19   52-63).

20   Regarding claims 14-15 and 27-28, Davis disclosed that the network is a public or private

21   network (See Davis Col. 6 Line 65 – Col. 7 Line 3).

1   Regarding claims 16 and 31, Davis disclosed that said communications pipe is provided

2   with a secure communications protocol (See Davis Col. 13 Lines 59-61 and Col. 20 Paragraph

3   1).

4   Regarding claim 24, Davis disclosed using a unique identifier associated with said PSD

5   for generating or retrieving said HSM cryptographic means (See Davis Col. 15 Line 63 – Col. 16

6   Paragraph 2).

7   Regarding claim 25, Davis disclosed using a unique identifier associated with said PSD

8   for retrieving said data or configuration changes (See Davis Col. 12 Paragraph 1).

9   Regarding claim 26, Davis disclosed that at least one command executable by said at

10   least one functional application is issued by said at least one HSM, routed through said

11   communications pipe into said PSD, and processed by said at least one functional application

12   (See Davis Col. 16 Paragraph 2).

13   *Claim Rejections - 35 USC § 103*

14   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

15   obviousness rejections set forth in this Office action:

16   *A patent may not be obtained though the invention is not identically disclosed or*
17   *described as set forth in section 102 of this title, if the differences between the subject matter*
18   *sought to be patented and the prior art are such that the subject matter as a whole would have*
19   *been obvious at the time the invention was made to a person having ordinary skill in the art to*
20   *which said subject matter pertains. Patentability shall not be negatived by the manner in which*
21   *the invention was made.*
22

23   Claims 5, 6-7, 17-18, 21-23, and 29-30 are rejected under 35 U.S.C. 103(a) as being

24   unpatentable over Davis.

1   Regarding claims 5 and 21, Davis disclosed a first and second server communicating

2   information (See Davis Fig. 4) but did not specifically disclose that they had the capability of

3   being mutually authenticated. However, mutual authentication between two communicating

4   network elements was well known in the art at the time of invention and therefore it would have

5   been obvious to provide the two devices with the ability of mutual authentication. This would

6   have been obvious because the ordinary person skilled in the art would have been motivated to

7   protect against illicit access to the contents of the devices.

8   Regarding claim 22, Davis disclosed using a unique identifier associated with said PSD

9   for mutually authenticating said PSD and said first server (See Davis Col. 13 Line 47 – Col. 14

10   Line 39).

11   Regarding claims 6-7, and 23, Davis disclosed using a functional application (See Davis

12   Col. 7 Lines 4-6), but did not specifically disclose that the application was identified by a unique

13   identifier. However, it was well known at the time of invention that applications had unique

14   names which were used to identify them. Therefore, it would have been obvious for the

15   application of Davis would have had a unique identifier used to identify the application.

16   Regarding claims 17-18 and 29-30, Davis disclosed encrypting the signatures in the

17   communications (See Davis Col. 13 Lines 59-61), but failed to disclose the type of encryption

18   used. However, both asymmetric and symmetric encryption were well known in the art at the

19   time of invention and therefore it would have been obvious to the ordinary person skilled in the

20   art at the time of invention to have used either.

1   Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis as applied to

2   claim 1 above, and further in view of DiGiorgio et al (US Patent Number 6,385,729) hereinafter

3   referred to as DiGiorgio.

4   Davis disclosed sending commands to a smartcard from the security card (See Davis Col.

5   14 Paragraph 3), but failed to disclose that the commands were APDU commands.

6   DiGiorgio teaches that APDUs are a standardized way to used to send commands to

7   token devices (See DiGiorgio Col. 9 Paragraph 1).

8   It would have been obvious to the ordinary person skilled in the art at the time of

9   invention to employ the teachings of DiGiorgio in the command system of Davis by sending the

10   commands to the stored-value card using APDUs. This would have been obvious because the

11   ordinary person skilled in the art would have been motivated to follow the standard way of

12   sending commands to a token device.

13   *Conclusion*

14   Claims 1-31 have been rejected.

15   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

16   policy as set forth in 37 CFR 1.136(a).

17   A shortened statutory period for reply to this final action is set to expire THREE

18   MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

19   MONTHS of the mailing date of this final action and the advisory action is not mailed until after

20   the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

21   will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

22   CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

1   however, will the statutory period for reply expire later than SIX MONTHS from the mailing

2   date of this final action.

3   Any inquiry concerning this communication or earlier communications from the

4   examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
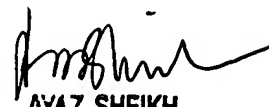
5   The examiner can normally be reached on M-F 8-4.

6   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

7   supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

8   organization where this application or proceeding is assigned is 571-273-8300.

9   Information regarding the status of an application may be obtained from the Patent

10   Application Information Retrieval (PAIR) system. Status information for published applications

11   may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

12   applications is available through Private PAIR only. For more information about the PAIR

13   system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

14   system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

15   like assistance from a USPTO Customer Service Representative or access to the automated

16   information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

17
18
19
20

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

21   Matthew Henning
22   Assistant Examiner
23   Art Unit 2131
24   7/25/2006

25